IBM Database Encryption Expert
December 2007

Information Management software

IBM Database Encryption Expert: Securing data in DB2

Contents

3 Data security — A top priority for all organizations

3 Introduction

4 Compliance and its effect on data security

6 The need for data access control

6 Data security threats

8 Solving the data security problem

8 Defense in depth

8 Where data lives in a database environment

9 Data security threats and protective measures

9 Direct access to file and log file viewing/tampering

10 System administrator privilege abuse

10 Stolen/Lost media

11 Solution — IBM Database Encryption Expert

11 IBM Database Encryption Expert architecture

12 Database Encryption Expert security policy overview

14 Database Encryption Expert policy management — The basics

15 Database Encryption Expert policy management — Process assignment

16 Using encryption to protect data-at-rest

17 Data security overview

18 Online data protection overview

21 Encrypted backup overview

22 Key management overview

23 Symmetric vs. asymmetric key encryption

24 Key management — Online data security use cases

25 Key management — Offline data security uses cases

26 Key management — Key protection

27 Summary

Data security—A top priority for all organizations

Introduction

Data security has become a critical issue for executives at the highest level of all organizations. Responding to this need, IBM offers Database Encryption Expert, which is designed to secure one of the most important assets any organization has – its data. Database Encryption Expert extends the capabilities of DB2® and related IBM data governance tools to provide the highest level of data security possible.

An active market for all types of stolen and compromised data has emerged. Private financial data, intellectual property, trade secrets, and classified government information have become targets. Due to increased threats to private and confidential data and increasing regulatory compliance pressure, organizations of all types are making the protection of their confidential data, as well as any private customer data they have, a top priority.

Regulators and the private sector are working to establish a framework of guidelines, legislation and regulations designed to require those who hold private/confidential data to protect it. The State of California was at the forefront with the passing of California Senate Bill 1386 (SB-1386), which requires any organization that experiences a data breach to notify all California residents who were affected. Since the passing of this bill into law, over 32 other states and some foreign governments have enacted similar legislation or are in the process of doing so.

The private sector, with real or potential out-of-pocket losses at stake, is taking regulation a step further. The Payment Card Industry Security Standards Council, a consortium comprised of Visa, MasterCard, American Express, and Diners Club, created a data security standard known as PCI DSS (Payment Card Industry Data Security Standard). It assesses penalties and fines, and may take other punitive measures against member organizations (for example, when a member organization loses cardholder data).

This paper explores the need for improved data security, describes basic security principals including encryption, and presents IBM Database Encryption Expert as a must-have tool in the data security framework.

Compliance and its effect on data security

Due to the increasing rate of data breaches, there has been an increase in regulatory compliance activity that focuses on data security. Governments and private industry have intervened in an attempt to prevent data breaches and to ensure data privacy. Compliance is a major force that is driving organizations to secure sensitive data.

Data security and the related protection of private/confidential data has become good business practice, and in many cases there are laws and regulations designed to ensure that all types of organizations are being diligent in ensuring that private/confidential data is strongly protected.

The following table contains a representative sampling of data-security-focused regulations and legislation:

Regulation	Purpose
Sarbanes-Oxley Act of 2002	• Designed to prevent corporate and accounting scandals • CEO and CFO certifications of annual and quarterly SEC reports • **Evaluation of the effectiveness of internal controls including those that ensure the integrity of financial data** • Rapid disclosure of material changes in financial conditions or operations • Establishes automatic controls repository to identify deficiencies
Gramm-Leach-Bliley Act	• Act passed to legalize mergers between banking and insurance companies • **Financial institutions are required to have a policy to protect information from security threats and data integrity** • Financial Privacy Rule requires financial institutions to provide a privacy notice to their customers every year • **Safeguards rule: Financial institutions should have a security plan to protect their consumers' non-public personal information** • **Pretexting protection: Financial institutions have to protect their consumers' non-public information by preventing someone without authority from accessing the information**
Health Insurance Portability and Accountability Act (HIPAA)	• Prevent unapproved access to patient treatment and payment information • **Protect patient data**
Basel II (primarily banking)	• Capital requirements should be more risk sensitive • Ensure the stability of individual banks and the banking system
Japanese Protecting Personal Information	• **Act on the Protection of Personal Information** • Personal information includes any information that can identify an individual (name, date of birth, etc.) • The person's consent is needed before someone can access his/her personal information
Financial Services and Markets Act (FISMA)	• Ensures consumers are protected • Insurance, banking or investment business need to be authorized before they can conduct regulated activities
Payment Card Industry (PCI)	• **Used to protect the cardholders' information** • **Access to cardholders' information will be restricted on a business need-to-know basis** • **All access to cardholders' information and network resources will be tracked and monitored** • Will maintain information security

The need for data access control

Data security is about controlling access to data. Those entities that should have access—users, applications and processes—are granted permission, while those entities that shouldn't are prevented from accessing the data.

Data access control has to be at the core of any viable data security solution. When data access control is used in conjunction with other security measures such as encryption, data governance tools, network and endpoint security devices, and most importantly, effective business practices, it can help complete the in-depth security infrastructure.

Access control is and has been an integral component of operating systems, applications, databases, and networks for many years. What was missing was data access control. Because data is a highly valuable asset, it makes sense that data should be included in the access control model. The challenge is how to make the data easily available to those that should have it while restricting those who shouldn't. Effective data-level access controls coupled with high-performance encryption can provide an optimal solution to ensure that an organization's private and confidential data is strongly protected.

Data security threats

Originally networks were closed, and the threats were relatively few. Some of the first security threats were viruses. Shortly thereafter, hackers emerged who accessed computing resources without permission and did so mainly for bragging rights. Hackers defaced Web sites and wrote malicious replicating code that could gain privileged access to key computing resources. It didn't take long, however, for the criminal element to see the opportunity in private/confidential data. Credit cards, social security numbers, and other personally identifiable information (PII) have market value to those who want to steal products, money or identities.

The following table lists some common threats and some of the corresponding protective measures.

Threat	Encryption	Host Access Control	Audit & Forensics
Root/System User	x	x	x
Direct Access to File	x	x	x
Unauthorized Viewing/ Logfile Tampering	x	x	x
Stolen/Lost Media	x		
Access by Unauthorized Application		x	x

In summary the key drivers behind improving data security are:

1. *Regulations and compliance – requirements for conducting business*
2. *Cost associated with data loss – the direct and indirect costs can be substantial*
3. *Reputation risk – bad publicity from a data breach*
4. *Protection of intellectual property for competitive reasons*

Private/confidential data must be protected regardless of whether it resides in online or offline environments. IBM Database Encryption Expert can help all types of organizations mitigate the risks that are associated with the loss or compromise of private/confidential data.

Awareness has grown in the wake of a number of highly visible and costly data breaches. Many organizations now understand that data security is a part of doing business and sometimes even provides a competitive advantage. Either way, organizations now view improved data security as an integral part of their regulatory compliance-driven business model.

Solving the data security problem

Defense in depth

Data security is constantly evolving as the threat model changes and becomes more intense. Threats to sensitive data can come from internal sources – such as administrators abusing their privileged access rights – as well as from external sources such as hackers penetrating perimeter and network security defenses to access private/confidential data. Securing data requires constant vigilance and a *defense in depth* data strategy. Defense in depth simply means the use of multiple security technologies and processes to deal with specific threats that when combined together protect against a broad range of those threats.

The defense in depth strategy requires a holistic view of data security. All points of access to data, systems, and processes need to be evaluated in relation to the threats against them and the vulnerabilities addressed. This process generally consists of the following phases:

1. *Understanding where all the data is and who/what accesses it*
2. *Identifying both internal and external threats*
3. *Implementing protective measures*

Where data lives in a database environment

An important first step in protecting data is knowing where it lives. Beyond the obvious are the many more obscure locations that need to be considered when developing a comprehensive data security strategy. The following list summarizes typical locations where sensitive data is found:

DB2 containers	ETL	Testing/QA extracts
Buffer pools	ODS	User/ Password files
Exports	Archive/ Hierarchical storage/Tape	History files
Spreadsheets	Logs	Diagnostic
Data warehouses	Replicated disks	OS temp/Swap files
Data marts	Mirrors	

Some locations such as spreadsheets and extracts live outside the boundaries of the controls available to the database. However, they illustrate the need for a comprehensive assessment and data protection strategy.

Data security threats and protective measures

Direct access to file and log file viewing/tampering

Unauthorized access to tablespaces and/or log files is a database environment threat that must be addressed. An attacker with root privilege can install applications that circumvent DBMS access controls and logging, and compromise data accessed by databases. An effective solution must:

1. *Create policies that tie the DBMS logging process to the log files and ensure that only the DBMS logging process can write to the log files and that the log files are encrypted*
2. *Protect the DBMS tablespaces by encrypting tablespace data*
3. *Grant full access only to authorized processes and encrypt the files*
4. *Block access from unauthorized applications*

These measures will prevent unauthorized applications, including malware, from being able to compromise file and log file information. These measures not only prevent access to data from any point except via legitimate means, such as the front end of the DBMS, but also prevent the log files from being manipulated. Log files that are protected by Database Encryption Expert can have audit integrity. Even someone with DBA privilege cannot tamper with the logs.

System administrator privilege abuse

System administrators have super-user access to the servers that they manage. System administrators of UNIX® systems can even use the SU command to pose as a legitimate process/user.

IBM Database Encryption Expert can control Sys Admin access to data in two ways:

- *Encrypt the data while leaving the metadata untouched – when data is encrypted, even direct access to a file is rendered meaningless.*
- *Restrict use of file system commands – control what file system commands are available to system users including the viewing of a file, directory or path. System administrators can be granted the privilege of maintaining server availability without being given access to or the ability to view the contents of sensitive files.*

This capability extends to the would-be attacker who attempts to gain administrative/root privilege through whatever means. Database Encryption Expert enforces the authentication of users who attempt to access protected files. It can force the user/administrators to authenticate through the authentication module (e.g. PAM, LAM). If proper credentials are not presented, access is denied.

Stolen/Lost media

The method of protecting data on removable media is simple: encryption. Database Encryption Expert provides high-performance encryption, which makes it practical to encrypt all data that will be stored on removable media.

Solution—IBM Database Encryption Expert

The data security marketplace has many different solutions that take a variety of approaches. IBM Database Encryption Expert combines the following aspects of data security:

- *High-performance encryption*
- *Data-level access controls*
- *Protection of data in both online and offline environments*
- *Unified and centralized policy and key management*

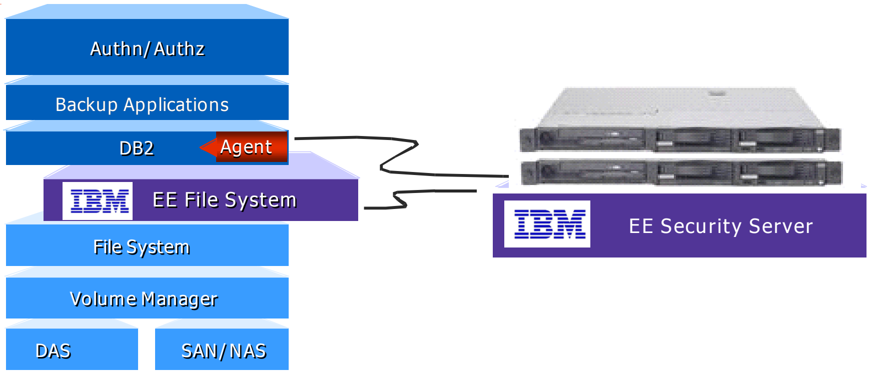
By using IBM Database Encryption Expert security policies, organizations can restrict access to data to only those users, applications and processes that should have it. The security policies can mirror an organization's guidelines for data access privileges.

IBM Database Encryption Expert architecture

Database Encryption Expert is a two-component solution comprised of one or more software Security Servers and DB2 Agents. The Security Server acts as the centralized point of administration for encryption key, data security policy and audit log collection.

Database Encryption Expert currently has two agents:

- *Online Data Protection Agent provides encryption services and access controls for data in online storage accessed by file systems.*
- *DB2 Agent provides encryption services for data being backed up to offline storage–both disk and tape.*



An important distinction between Database Encryption Expert and other solutions that offer encryption is how the encryption is performed. Database Encryption Expert employs a technique in which the file metadata is left in clear text (unencrypted) while the file contents are encrypted. This technique provides an additional level of file access control in addition to what the file system offers – access without viewability. Effectively, an application can be granted access to a file for the purposes of management without decrypting its contents. Privileged super users can continue to manage their environments and access the file, but be restricted from having clear-text access to the file content. This capability helps mitigate risks from internal malicious activity targeted at private/confidential data.

Database Encryption Expert security policy overview

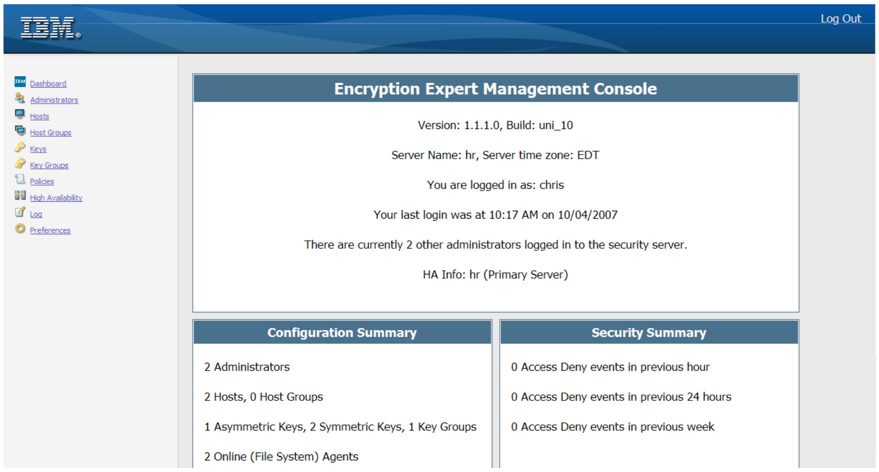
Security policies are at the core of Database Encryption Expert.

They control:

- *Who and what can access data*
- *When data can be accessed*
- *Where data can be accessed from, and*
- *How data is accessed*

Policies also control the use of encryption keys and what events are logged (e.g. all file accesses, policy violations, etc.). These data security policies allow organizations to translate business rules into data access control and protection policies.

The policy engine is managed via a browser interface hosted from the Security Server. From one Security Server the policies for many database servers and Database Encryption Expert agents can be managed. Geographical proximity is not a restriction as long as there is IP connectivity between the Database Encryption Expert agents that reside on DB2 database servers and the Security Server. It is possible (in fact, it is a best practice) to cluster the Security Servers for high availability and failover.



Encryption Expert Management Console

Version: 1.1.1.0, Build: uni_10

Server Name: hr, Server time zone: EDT

You are logged in as: chris

Your last login was at 10:17 AM on 10/04/2007

There are currently 2 other administrators logged in to the security server.

HA Info: hr (Primary Server)

Configuration Summary

2 Administrators

2 Hosts, 0 Host Groups

1 Asymmetric Keys, 2 Symmetric Keys, 1 Key Groups

2 Online (File System) Agents

Security Summary

0 Access Deny events in previous hour

0 Access Deny events in previous 24 hours

0 Access Deny events in previous week

Database Encryption Expert policy management—The basics

The most fundamental tenet of a data security policy is an association between a process and a file. The process represents an application, and the file represents the data.

Once this association is established, data access privileges via Database Encryption Expert policies are assigned. Privileges include all file system operations that are available for a given platform, such as file open, close, delete, etc., plus the ability to view file contents. The ability to grant file access without the ability to view its contents is a function of Database Encryption Expert's method of encryption.

Database Encryption Expert does not supersede operating system privileges; it supplements them. If a user does not have operating system rights to a directory or file, then Database Encryption Expert policies will not be able to grant it. If, however, the operating system grants access, but the Database Encryption Expert policy does not, then access is denied. In essence, you can think of this capability as a data security extension of operating system/file system access controls and control lists.

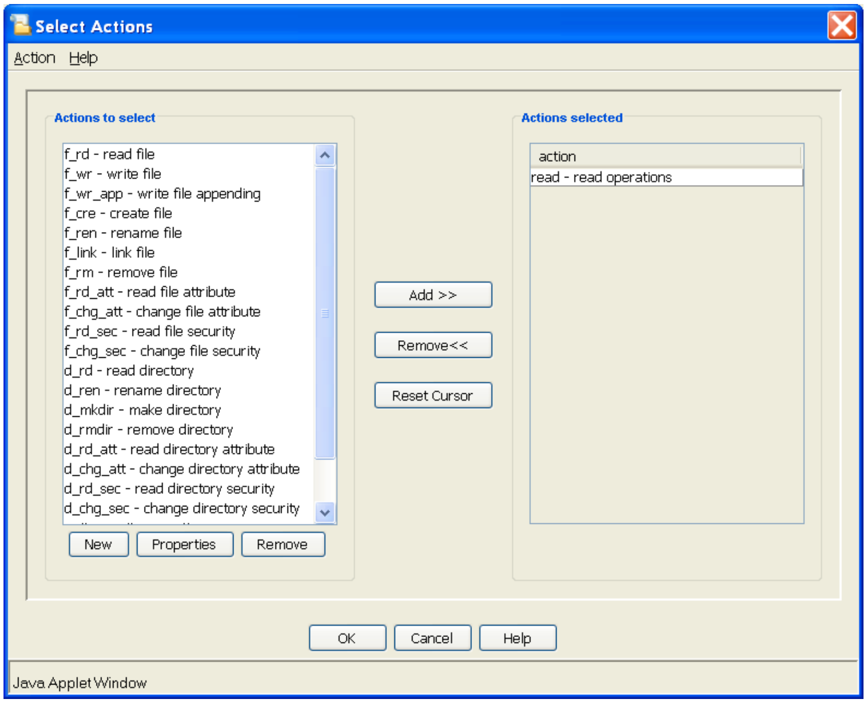
The rules in Database Encryption Expert operate very much like those in a firewall. Rules are ordered and matched in a predetermined way, e.g. first matched. There is considerable flexibility in the way Database Encryption Expert rules are processed. The recommended best practice is to implement the policies incrementally. It is important to remember that Database Encryption Expert protects data – encrypts it – as well as controls access to it.

The most basic policy would simply state that all files within a tablespace should be encrypted, thereby protecting those files. If controlling access to the files in the tablespace is required, access control rules could be added to the encryption policy. The combination of access controls and encryption would ensure comprehensive protection of the files in the tablespace.

Database Encryption Expert policy management—Process assignment

The concept of tying a process to a file and assigning privileges has the inherent benefit of restricting access to data only from authorized processes. The Database Encryption Expert security administrator decides in advance what processes can access a file and what level of access those processes should have.

The following screen shot from the Database Encryption Expert security administrator interface shows the file and process controls that are available.



f_rd - read file
f_wr - write file
f_wr_app - write file appending
f_cre - create file
f_ren - rename file
f_link - link file
f_rm - remove file
f_rd_att - read file attribute
f_chg_att - change file attribute
f_rd_sec - read file security
f_chg_sec - change file security
d_rd - read directory
d_ren - rename directory
d_mkdir - make directory
d_rmdir - remove directory
d_rd_att - read directory attribute
d_chg_att - change directory attribute
d_rd_sec - read directory security
d_chg_sec - change directory security

action
read - read operations

Database Encryption Expert recognizes processes based on their name and path. The following table lists some key DB2 processes with access controls.

Process	Description	File	Privilege
Db2syslog	Logging	Log files	View, O, R/W
Db2sysc	System Controller	Tablespaces	View, O, R/W, D
Pfchr	Buffer pool pre-fetcher	Buffer pool	View, R/W
Db2pclnr	Page cleaner	Page space	View, R/W, D
O=Open, D=Delete, R/W=Read/Write			

Using encryption to protect data-at-rest

While logical file access permissions may control access via the host, encryption provides physical protection of the data-at-rest in storage.

Note—Database Encryption Expert can protect files via data-level access controls and encryption in the following storage environments through the use of its unified and centralized policy/key management and related encryption services:

- *Tapes*
- *Offline media*
- *NAS*
- *SAN*
- *DAS*

Database Encryption Expert provides the means to encrypt files and even entire volumes. Encryption is especially important when files are stored on a network device. Since network storage usually supports many clients, there may potentially be multiple access points or nodes that can access files, and as such are beyond the protection of the operating and file system controls. Also, encryption is very effective for protecting data on removable media such as tapes.

Encryption in the Database Encryption Expert model is effectively an attribute of the data security policies that are established by the data security administrator. Once the process-file association is defined and access rights are established, encryption on a file-by-file basis can be enabled. The encryption used is the Advanced Encryption Standard (AES). The security administrator then chooses the strength of the encryption key, either 128 or 256 bytes, and gives the key a name. Usually the key name has some relevance to the data being protected. The actual encryption keys are never revealed to the security administrators, systems administrators or DBAs.

Data security overview

Effective data security should mitigate risks against a broad range of threats – both internal and external. Database Encryption Expert does this by combining high-performance encryption with access controls:

- *Encryption provides physical protection of the data.*
- *Access control restricts the who, what, when, where and how data can be accessed through the database server.*

Database Encryption Expert can use one or a combination of the above controls to strongly protect data and mitigate risks from both internal and external attacks.

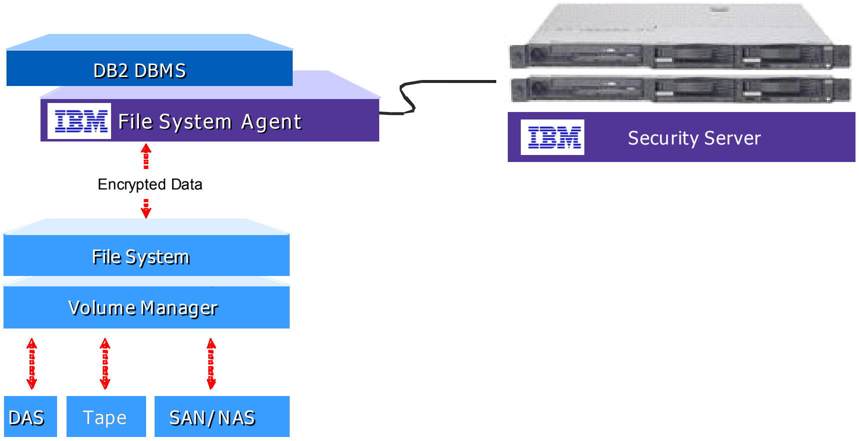
Online data protection overview

The Database Encryption Expert online agent is installed on the database server where access to data needs to be controlled. The online agent works by intercepting calls to the file system as a proxy file system, comparing those requests to data security policy and acting accordingly. The online agent also performs the cryptographic operations (encryption/decryption) and enforces the access control policies. The online agent is a stackable file system on UNIX platforms.

When Database Encryption Expert is combined with:

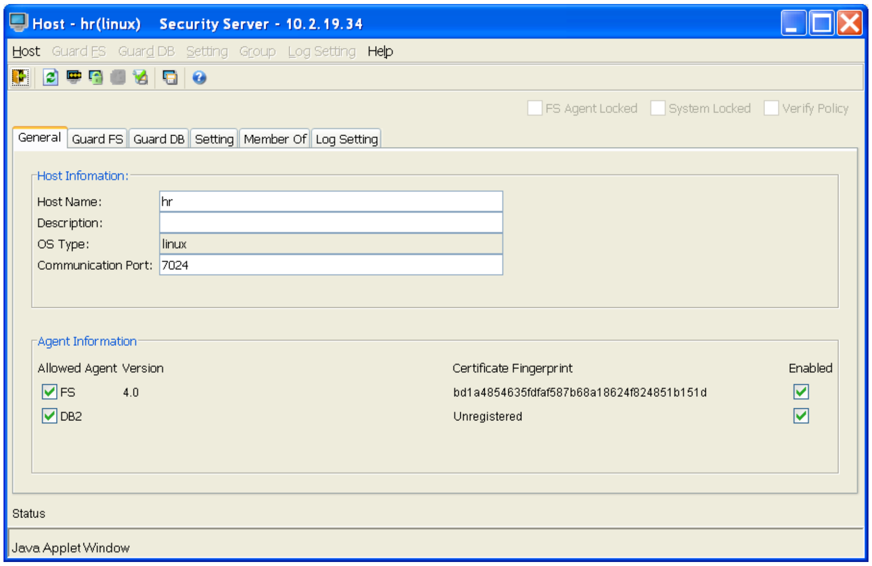
- *Native operating system access controls*
- *Directory services and authentication*
- *Native DB2 controls, such as Label-Based Access Control*
- *Other IBM data governance tools*

The result is a highly effective data security solution that meets an organization's data governance and compliance needs.



The cryptographic operations (encryption/decryption) are executed by the online agent. Database Encryption Expert utilizes AES libraries that have been optimized to operate in a multi-threaded environment. When a file system request is presented to the agent, it is evaluated against the rules in the security policy. The policy determines what key to use and the data is encrypted or decrypted using the designated key. The stream is then passed to the underlying file system. The advantage of this approach is that it operates transparently to users, applications, the DB2 database, the network and the storage infrastructure where the protected data resides. DB2 has no knowledge that Database Encryption Expert is operating underneath it. As far as DB2 is concerned, it makes file system calls and is serviced just as it always was – and there is no need to change DB2 database structure and schema. This provides optimal transparency and performance.

This first step in protecting online data is to select a host, i.e., the DB2 server that accesses the data to be protected.



□ FS Agent Locked □ System Locked □ Verify Policy

Host Infomation:

Host Name: hr
Description:
OS Type: linux
Communication Port: 7024

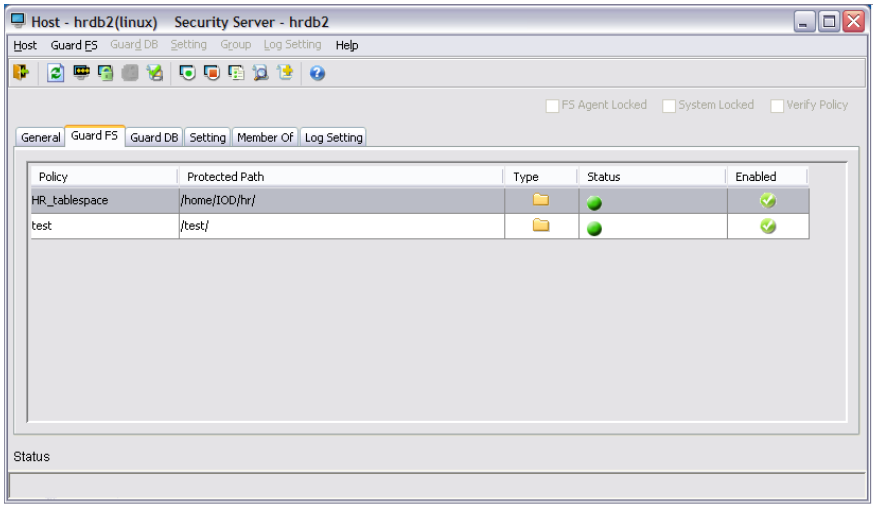
Agent Information

Allowed Agent	Version	Certificate Fingerprint	Enabled
☑ FS	4.0	bd1a4854635fdfaf587b68a18624f824851b151d	☑
☑ DB2		Unregistered	☑

Status

Java Applet Window

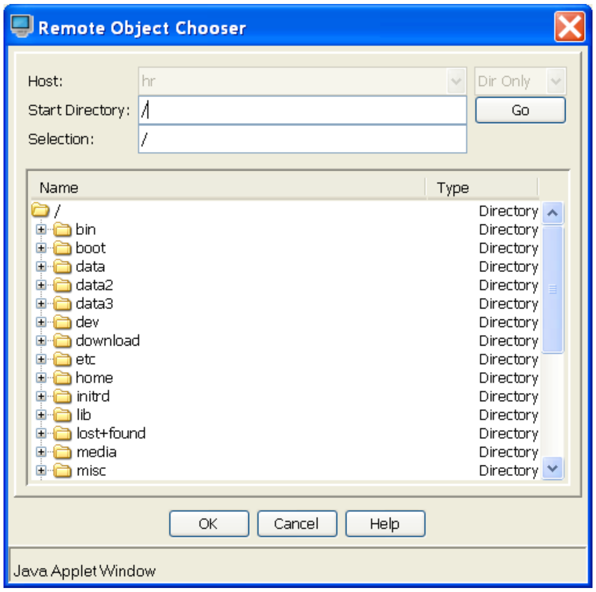
The second step is to define a Guard Point.



□ FS Agent Locked □ System Locked □ Verify Policy

Policy	Protected Path	Type	Status	Enabled
HR_tablespace	/home/IOD/hr/	📁	●	✓
test	/test/	📁	●	✓

The Guard Point specifies the location where the files/data to be protected reside.



Host: hr
Dir Only
Start Directory: /
Selection: /

Name	Type
/	Directory
bin	Directory
boot	Directory
data	Directory
data2	Directory
data3	Directory
dev	Directory
download	Directory
etc	Directory
home	Directory
initrd	Directory
lib	Directory
lost+found	Directory
media	Directory
misc	Directory

Once the Guard Point is activated, the data security policies can be composed.

Encrypted backup overview

The Secure Backup agent operates as an application callout. It interfaces with the DB2 compression API and is invoked when the DBA initiates a backup. The backup job is compared to data security policy and the data is either encrypted using the key prescribed in policy or is left untouched and returned to DB2.

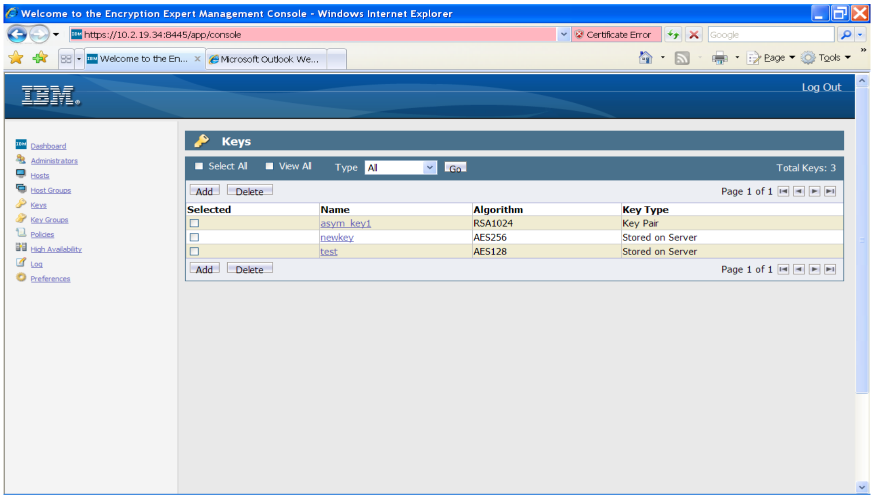
Using Database Encryption Expert to protect backups requires no changes to the downstream backup process. Whatever backup application or storage infrastructure is used remains unchanged. The only difference is in how the backup processing is handled once the DBA initiates the process.

As with the online agent, all encryption is executed in software on the database server with minimal performance impact. In addition to encryption, the secure backup agent can provide compression services as well. The only requirement is the compression takes place before the encryption. The reason is simple: the compression algorithm looks for patterns in the data. Encryption seeks to remove all patterns.

Many organizations utilize tape drive compression. In most cases, it is not necessary to turn the compression off at the drive. Current tape drives have intelligent compression engines that sample the effectiveness of the compression and self regulate (turn compression on and off).

Key management overview

Whenever encryption is used, key management becomes an important and integral component of the data security solution. Key management in Database Encryption Expert is handled by the key management component of the Security Server. The data security policies established by the Database Encryption Expert administrator govern the use of the encryption keys, which subsequently govern access to the file data.



Welcome to the Encryption Expert Management Console - Windows Internet Explorer

https://10.2.19.34:8445/app/console

Certificate Error

Keys

□ Select All □ View All Type: All

Total Keys: 3

Page 1 of 1

Selected	Name	Algorithm	Key Type
□	asym_key1	RSA1024	Key Pair
□	newkey	AES256	Stored on Server
□	test	AES128	Stored on Server

Page 1 of 1

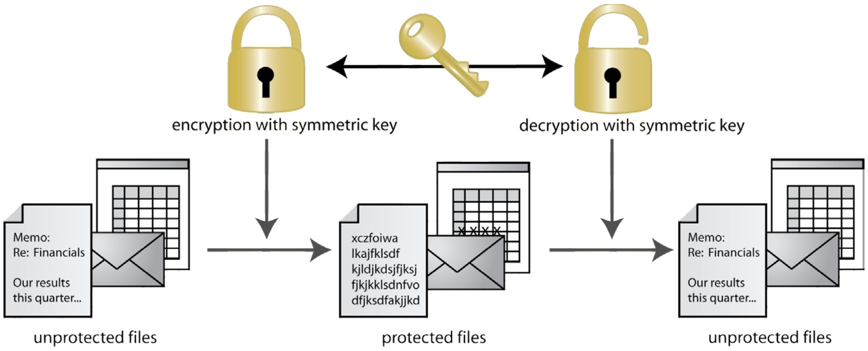
Because the key management is largely a function of the security policy, the mechanics of Database Encryption Expert key management are hidden, making key management administratively simple and secure.

Database Encryption Expert utilizes both symmetric keys and asymmetric (public/private) key pairs. The symmetric keys are used for the encryption of the file data whether online or offline. Asymmetric keys are used to wrap the symmetric keys that are used for DB2 secure backups (key encrypting keys) and to protect the symmetric and private keys that are stored in the Security Server. Symmetric key encryption has higher performance and is subsequently used to encrypt the file data. Asymmetric encryption is used for the distribution of data, as in the case of backups. Asymmetric encryption allows Encryption Expert to support a broader range of business use cases including allowing third parties to decrypt the data.

Symmetric vs. asymmetric key encryption

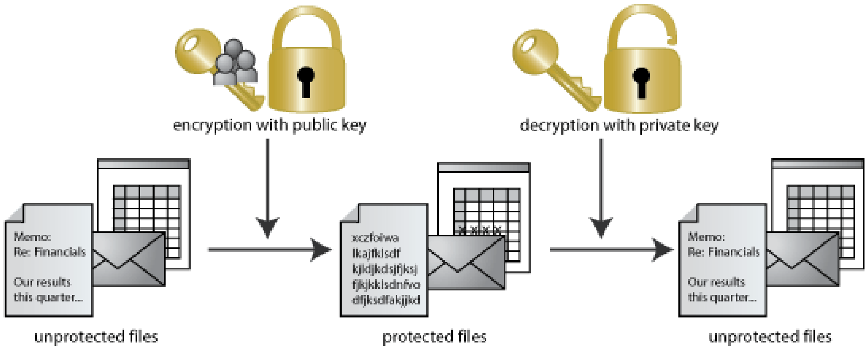
Symmetric key cryptography uses the same key to encrypt data (lock) as it does to decrypt data (unlock). Database Encryption Expert utilizes the Advanced Encryption Standard (AES) algorithm, either 128 or 256 bits for all symmetric key operations. The advantage is performance. AES is optimized for use on

general purpose processors and is the algorithm recommended by the National Institute for Standards and Technology (NIST).



Asymmetric key cryptography has two components: a public key and a private key. Historically, it has been known as PKI or public key infrastructure. In the case of encryption, data is encrypted using the public key and decrypted with the private key. The public key can be made freely available, and data is encrypted such that only the possessor of the private key can unlock the data.

Database Encryption Expert uses asymmetric encryption to create key envelopes used in secure backup and restores and to protect the keystore (database) in the Security Server.

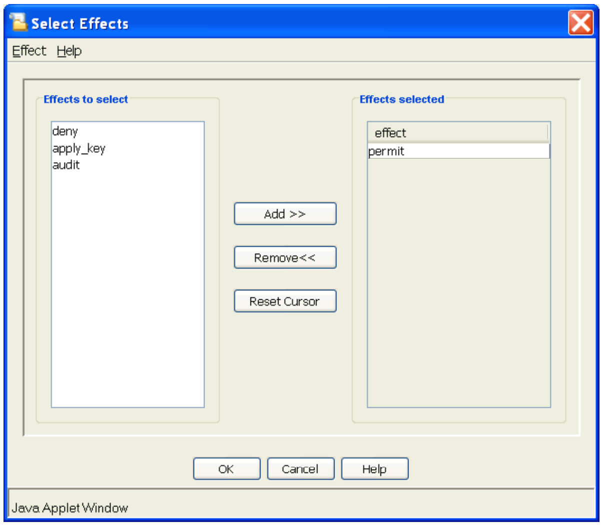


Key management—Online data security use cases

Online database files are typically accessed frequently and tend to be larger in size. They also happen to be the files that support business applications such as SAP and as such have a requirement of high availability and system performance. The encryption of online files is best served with symmetric encryption keys and processing. This is the approach that Database Encryption Expert uses.

Although different keys can be assigned to individual files, most organizations should use one key per directory or volume. The exception is when files are in a shared directory/volume and encryption is used to compartmentalize them. That way, for instance, different departments such as finance and engineering can co-mingle their files while being assured that only authorized users and applications can view them. DB2 partitions can also be cryptographically separated by assigning unique keys to each partition.

Database Encryption Expert security policy treats encryption as an effect. What that means is that the policy defines for whom a file is decrypted. A file can alternatively be presented to the requester in cipher text (still encrypted). That way, an individual/process can be granted the right to manage a file without the ability to view its contents. Effect is defined once a key is associated with a policy.



Key management—Offline data security use cases

A variety of business-use cases must be covered for an effective encrypting backup and restore solution. As with traditional backups, it is the ability to restore that is critical. Database Encryption introduces the concept of a restore rule and enhances not only the security of the product but also its ability to address core business needs.

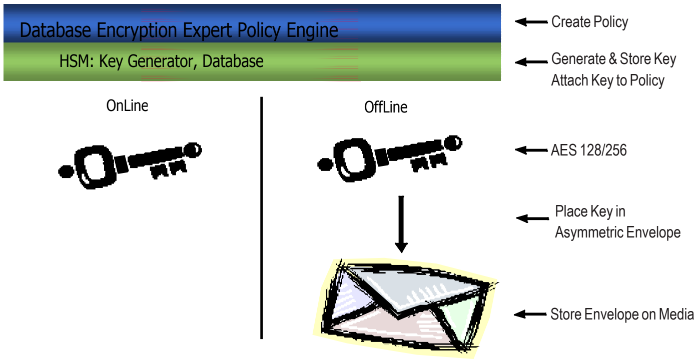
The following scenarios are supported:

1. *Backup and restore to the primary site*
2. *Backup and restore to a preconfigured business continuity site*
3. *Backup and restore to a pre-designated but not necessarily configured business continuity site such as a third-party business continuity facility*
4. *Restore at an affiliate location*

The restore rule is possible because the Database Encryption Expert security policies provide the rule framework, and the symmetric keys that are used to encrypt the data are stored with the backup and wrapped in an asymmetric envelope (key encrypting key).

The public key that is used to create the envelope can be that of the organization that creates the backup or an affiliate (third party). Only those who possess the private key can open the envelope and decrypt the backup.

The following diagram depicts the symmetric and asymmetric key management that is available in Database Encryption Expert.



Key management—Key protection

Encryption keys are critical data and must be protected and always available. The encryption keys in Database Encryption Expert are stored in a DB2 database within the Security Server and are themselves encrypted.

Availability is maintained using replication across the Security Server cluster.

Note—Being critical to data availability, it is a best practice and highly recommended that the encryption keys, key indexes and policies be backed up from the Security Server and stored securely. If the keys are lost, so is the data.

Because of where the secure backup agent sits architecturally, it is able to recognize the context of the database environment. The following elements are made available to the security policy composer and govern the secure backup process:

- *Agent host name*
- *DB2 database alias*
- *DB2 database partition number (DB2 9.x only)*
- *DB2 database instance name*
- *Permissible time range, relative to the Security Server*

Database Encryption Expert securely stores the symmetric keys that are used to encrypt the data on the media with the data. This approach, which is also employed by the IBM TS1120 encrypting tape drive, provides maximum flexibility in choosing how or where a backup is restored without exposing the organization to unnecessary risk.

One must have the private key to unlock the data. The private key is protected by the security server or the affiliate receiving the data.

Summary

Data security is a complex, ever changing and critical discipline. The threats to data are many and constantly evolving. IBM Database Encryption Expert is a proven data security solution for mitigating the multitude of threats targeting private/confidential data. Combining high-performance encryption with data-level access control, in addition to DB2 security features, results in a tightly controlled and secure database and data environment.

Database Encryption Expert is easy to install and administer. Being policy driven and centrally managed, it provides the flexibility to operate in any organization and protect all types of data serviced by DB2.

Data security is no longer an afterthought. It is now required to be part of the core IT operation and infrastructure. IBM Database Encryption Expert can easily and transparently integrate into DB2 environments and meet an organization's data security and compliance needs. For additional information please visit the Database Encryption Expert Product Page at **ibm.com**/software/data/db2imstools/database-encryption-expert/ or the DB2 and IMS tools website at **ibm.com**/software/data/db2imstools/.

IBM Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
12-07

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

TAKE BACK CONTROL WITH Information Management